Amendment in Response to Examiner's Answer
Applicant: Alexander C. Ranous et al.
Serial No.: 09/560,032
Filed: April 27, 2000
Docket No.: 10002142-1
Title: INTERNET USAGE DATA RECORDING SYSTEM AND METHOD EMPLOYING A CONFIGURABLE RULE ENGINE FOR THE PROCESSING AND CORRELATION OF NETWORK DATA

IN THE CLAIMS

Amendments to the Claims

Please cancel claims 1-12, 17, 18, 24 and 25

Please amend claim 19 as follows:

1-12. (Cancelled)

13. (Original) A method for recording network usage including correlating of network usage information and network session information, the method comprising the steps of:

defining a network data correlator collector including an encapsulator, an aggregator, and a data storage system;

receiving a set of network session data via the encapsulator;

processing the network session data set via the aggregator, including the steps of defining a first rule chain and applying the first rule chain to the network session data to construct an aggregation tree;

receiving a set of network usage data via the encapsulator;

processing the network usage data set via the aggregator, including the steps of defining a second rule chain and applying the second rule chain to the network usage data and the aggregation tree to construct a correlated aggregation tree;

determining a correlated data set from the correlated aggregation tree; and

storing the correlated data set in the data storage system.

14. (Original) The method of claim 13, wherein the network session data set is in a standard data format received from a session data collector having an encapsulator, an aggregator and a data storage system.

15. (Original) The method of claim 14, wherein the network usage data set is in the standard data format received from a usage data collector having an encapsulator, an aggregator and a data storage system

16. (Original) The method of claim 13, further comprising the step of defining the first rule set to be different than the second rule set.

17. (Cancelled)

18. (Cancelled)

19. (Currently Amended) ~~The method of claim 18~~ A method for recording network usage comprising:

defining a first network data collector including a first encapsulator, a first aggregator, and a first data storage system;

receiving a first set of network data via the first encapsulator;

processing the first network data set via the first aggregator, including the steps of defining an aggregation rule chain and determining a first set of aggregated data by applying the aggregation rule chain to the first set of network data; and

storing the first aggregated network data set in the first data storage system, wherein the step of applying the aggregation rule chain to the first set of network data further comprises the steps of:

constructing an aggregation tree; and

determining the first aggregated network data set from the aggregation tree,

-wherein ~~the step of~~ constructing an aggregation tree further includes ~~the steps of~~:

defining the first network data set to includes a first network data event and a second

network data event;

applying the aggregation rule chain to the first network data event to construct a hierarchy of group nodes within the aggregation tree; and

applying the aggregation rule chain to the second network data event to locate similar

group nodes according to a predefined set of match rules, if no matching -group nodes exist, extending the hierarchy of group nodes within the aggregation tree by creating additional group nodes.

20. (Original) The method of claim 19, wherein the step of applying the aggregation rule chain to the first network data event further includes the steps of:

defining the aggregation rule chain to include a first match rule for matching source IP address;

defining the first network data event to include a first source IP address;

applying the first match rule to the first network data event, including determining whether the aggregation tree includes a first group node matching the first source IP address; and

if a matching first group node does not exist, creating the first group node for the first source IP address.

21. (Original) The method of claim 20, wherein the step of applying aggregation rule chain to the first network data event further includes the steps of:

defining the aggregation rule chain to include a second match rule for matching destination IP address;

defining the first network data event to include a first destination IP address;

applying the second match rule to the first network data event, including determining

whether the aggregation tree includes a second group node matching the first destination IP address; and

if a matching second group node does not exist, creating the second group node for the first destination IP address.

22. (Original) The method of claim 21, wherein the step of applying the aggregation rule chain to the first network data event further includes the steps of:

defining the aggregation rule set to include an aggregation rule;

defining the first network data event to include a port number and volume of information;

applying the aggregation rule to the first network data event, including copying the port number, source IP address, destination IP address and volume information to the second group node.

23. (Original) The method of claim 17, further comprising the steps of:

defining a second network data collector including a second encapsulator, a second aggregator, and a second data storage system;

receiving a second set of network data via the second network encapsulator;

processing the second network data set via the second aggregator, including the steps of defining a second rule chain and applying the second rule chain to the second set of network data to define a second set of aggregated network data; and

storing the second aggregated network data set in the second data storage system.

24. (Cancelled)

25. (Cancelled)

26. (Original) A network usage recording system having a network data correlator collector, the network data correlator collector comprising:

an encapsulator which receives a set of network session data;

an aggregator for processing the network session data set, the aggregator including a defined first rule chain, wherein the aggregator applies the first rule chain to the network session data set to construct an aggregation tree;

wherein the encapsulator receives a set of network usage data, and the aggregator processes the network usage data set, the aggregator including a defined second rule chain, wherein the aggregator applies the second rule chain to the network usage data set and the aggregation tree to construct a correlated aggregation tree, and determines a correlated data set from the correlated aggregation tree; and

a data storage system for storing the correlated data set.

27. (Original) The system of claim 26, wherein the network session data set is in a standard data format received from a session data collector having an encapsulator, an aggregator and a data storage system.

28. (Original) The system of claim 27, wherein the network usage data set is in the standard data format received from a usage data collector having an encapsulator, an aggregator and a data storage system.

29. (Original) The system of claim 26, further wherein the first rule set is different than the second rule set.

30. (Previously Presented) A method for recording network usage comprising:

defining a first network data collector including a first encapsulator, a first aggregator, and a first data storage system;

receiving a first set of network data via the first encapsulator;

processing the first network data set via the first aggregator, including the steps of defining an aggregation rule chain and determining a first set of aggregated data by applying the aggregation rule chain to the first set of network data; and

storing the first aggregated network data set in the first data storage system;

wherein applying the aggregation rule chain to the first set of network data further comprises:

constructing an aggregation tree; and

determining the first aggregated network data set from the aggregation tree;

wherein constructing an aggregation tree further includes defining the first network data set to includes a first network data event and a second network data event;

applying the aggregation rule chain to the first network data event to construct a hierarchy of group nodes within the aggregation tree; and

applying the aggregation rule chain to the second network data event to locate similar group nodes according to a predefined set of match rules, if no matching group nodes exist, extending the hierarchy of group nodes within the aggregation tree by creating additional group nodes;

wherein applying the aggregation rule chain to the first network data event further includes:

defining the aggregation rule chain to include a first match rule for matching source IP address;

defining the first network data event to include a first source IP address;

applying the first match rule to the first network data event, including determining whether the aggregation tree includes a first group node matching the first source IP address; and if a matching first group node does not exist, creating the first group node for the first source IP address;

wherein applying aggregation rule chain to the first network data event further includes:

defining the aggregation rule chain to include a second match rule for matching destination IP address;

defining the first network data event to include a first destination IP address;

applying the second match rule to the first network data event, including determining whether the aggregation tree includes a second group node matching the first destination IP address; and if a matching second group node does not exist, creating the second group node for the first destination IP address;

wherein applying the aggregation rule chain to the first network data event further includes:

defining the aggregation rule set to include an aggregation rule;

defining the first network data event to include a port number and volume of information;

applying the aggregation rule to the first network data event, including copying the port number, source IP address, destination IP address and volume information to the second group node.

31. (Previously Presented) The method of claim 30, further comprising:

defining a second network data collector including a second encapsulator, a second aggregator, and a second data storage system;

receiving a second set of network data via the second network encapsulator;

processing the second network data set via the second aggregator, including:

defining a second rule chain and applying the second rule chain to the second set of network data to define a second set of aggregated network data; and

storing the second aggregated network data set in the second data storage system.